Department of Defense
INSTRUCTION

SUBJECT: DoD Installation Emergency Management (IEM) Program

References: See Enclosure 1

1. <u>PURPOSE</u>. This Instruction, under the authority of DoD Directive (DoDD) 5134.01 (Reference (a)):

    a. Establishes policy, assigns responsibilities, and prescribes procedures for developing, implementing, and sustaining IEM programs at DoD installations worldwide for "all hazards" as defined in the glossary.

    b. Establishes the goals of the DoD IEM Program as follows:

        (1) Prepare DoD installations for emergencies.

        (2) Respond appropriately to protect personnel and save lives.

        (3) Recover and restore operations after an emergency.

    c. Aligns DoD emergency management (EM) activities with the National Incident Management System (NIMS), the National Preparedness Guidelines (NPG), and the National Response Framework (NRF) (References (b), (c), and (d)).

    d. Establishes the DoD EM Steering Group (EMSG).

    e. Authorizes other publications such as manuals to provide specific information on the DoD IEM Program.

2. <u>APPLICABILITY</u>. This Instruction applies to:

    a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other

		Form Approved
Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **19 NOV 2010**	2. REPORT TYPE	3. DATES COVERED **00-00-2010 to 00-00-2010**
4. TITLE AND SUBTITLE **DoD Installation Emergency Management (IEM) Program**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Washington,DC,20301-3400**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**49**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

b. All DoD ~~operations, activities, and~~ installations worldwide, including Government-owned, contractor-operated facilities and non-DoD activities operating on DoD installations.

c. All DoD personnel, including Active and Reserve Components, DoD civilians, DoD families, DoD and non-DoD tenants, transient DoD and U.S. Government personnel, and DoD contractors living and/or working on DoD installations worldwide.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy to:

a. Maintain DoD readiness by establishing and maintaining a comprehensive, all-hazards IEM Program on DoD installations worldwide.

b. Support and assist U.S. civil authorities, as directed, in EM activities for mitigating, preventing, planning for, responding to, and recovering from a natural or manmade disaster or hazard.

c. Adopt and implement procedures consistent with NIMS and the incident command system (ICS) in accordance with ~~the Deputy Secretary of Defense Memorandum~~ *Homeland Security Presidential Directive 5* (Reference (e)).

d. Adopt and implement, as appropriate, recommendations in Appendix A of Reference (c), IEM program management, emergency planning, and continuity planning.

e. Support the implementation of the NRF within the United States through the development, implementation, and sustainment of the DoD IEM Program detailed in this Instruction. For consistency and as a matter of practice, the guidelines set forth in Reference (d) will be implemented to the greatest extent possible at all U.S. installations outside the United States in accordance with Reference (e).

f. Coordinate preparedness, response, and recovery requirements and capabilities with State, local, and tribal governments; other Military Department(s); or host-nation partners using an all-hazards approach that balances risk management (i.e., threat, vulnerability, and consequence), resources, and need.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES

    a. Standards

      (1) Apply EM ~~requirements~~*standards* and best practices as issued in this Instruction and consider applicable EM ~~requirements~~*standards* and best practices issued by, for example, the Department of Homeland Security and the National Fire Protection Association (NFPA).

      (2) For procedures and policies at installations in non-U.S. locations, maintain consistency with national standards and guidelines to the greatest degree practical, except where compliance at such locations is mandated.
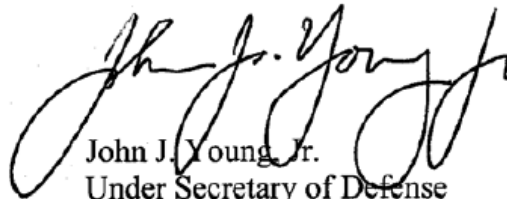
    b. Written Plan. Develop, implement, and maintain a written statement of policy that establishes, implements, and sustains the IEM Program.

    c. Minimum Program Requirements. Implement the IEM Program at installations using the requirements described in Enclosures 3 through 7.

    d. Liaisons. Any discussions, liaisons, negotiations, or other contacts with foreign governments or international organizations pursuant to the IEM Program shall be accomplished in coordination with the Under Secretary of Defense for Policy (USD(P)) and in strict compliance with all requirements governing contacts and agreements with foreign states or international organizations.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Instruction is effective immediately.

John J. Young, Jr.
Under Secretary of Defense
for Acquisition, Technology, and Logistics

Enclosures
    1. References
    2. Responsibilities
    3. DoD IEM Program Execution
    4. IEM Program Planning
    5. Preparedness
    6. Incident Response
    7. Recovery Phase
    Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a)   DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005
(b)   U.S. Department of Homeland Security, "National Incident Management System," March 1, 2004[1]
(c)   U.S. Department of Homeland Security, "National Preparedness Guidelines," September 2007[2]
(d)   U.S. Department of Homeland Security, "National Response Framework," January 2008[3]
(e)   ~~Deputy Secretary of Defense Memorandum, "Implementation of the National Response Plan and the National Incident Management System," November 29, 2005~~[4] *Homeland Security Presidential Directive 5, "Management of Domestic Incidents," February 28, 2003*[4]
(f)   DoD 3150.8-M, "Nuclear Weapon Accident Response Procedures (NARP)," February 22, 2005
(g)   DoD Directive 3150.*0*8, "DoD Response to ~~Radiological Accidents~~ *Nuclear and Radiological Incidents*," ~~June 13, 1996~~ *January 20, 2010*
(h)   Title 10, United States Code
(i)   Section 1522 of title 50, United States Code
(j)   DoD Directive 3020.40, "~~Defense Critical Infrastructure Program (DCIP)~~ *DoD Policy and Responsibilities for Critical Infrastructure*," ~~August 19, 2005~~ *January 14, 2010*
(k)   DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management," April 21, 2008
(l)   Civilian Personnel Management Service, "Emergency Preparedness and Response Guide," May 2007[5]
(~~l~~*m*)   DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(~~m~~*n*)   *U.S. Department of Homeland Security, "*Maritime Operational Threat Response Plan," October 2006*[6]
(~~n~~*o*)   *Maritime Security Policy Coordinating Committee,* ~~National Strategy for Maritime Security,~~ *"The* Maritime Infrastructure Recovery Plan *for the National Strategy for Maritime Security*," ~~October~~ *April* 2006[~~6~~7]

---

[1] Available from http://www.dhs.gov/xlibrary/assets/NIMS-90-web.pdf
[2] Available from http://www.dhs.gov/xlibrary/assets/National_Preparedness_Guidelines.pdf
[3] Available from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf
[4] Available from ~~https://www.denix.osd.mil/portal/page/portal/content/shf/References/ODSD Memo - NRP NIMS (29 Nov 05)_0.pdf~~ *http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm*
[5] *Available from http://www.cpms.osd.mil/ASSETS/E9CC9CEA4BA546B99EBF428CFCB9CA9F/Emergency%20Preparedness%20Guide.pdf*
[6] *Available to authorized users via the Defense SECRET Internet Protocol Router Network (SIPRNET) at https://clsobdom02.cno.navy.smil.mil/motr/*
[~~6~~7] Available from http://www.dhs.gov/xlibrary/assets/HSPD_MIRPPlan.pdf

(~~o~~*p*) National Fire Protection Association (NFPA) 1600, "Standard on Disaster/Emergency Management and Business Continuity Programs," 2007 Edition[7][8]

(~~p~~*q*) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006

(~~q~~*r*) U.S. Department of Homeland Security, Homeland Security Exercise and Evaluation Program (HSEEP), "Volume III: Exercise Evaluation and Improvement Planning," February 2007[8][9]

(~~r~~*s*) Federal Information Processing Standards Publication 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006[9][10]

(~~s~~*t*) Homeland Security Presidential Directive 12, "~~Policy~~ *Policies* for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004[10][11]

(~~t~~*u*) Federal Emergency Management Agency, Independent Study Program, Course IS-200.a, "Incident Command System (ICS) for Single Resources and Initial Action Incidents*,*" *current edition*[11][12]

(~~u~~*v*) Federal Emergency Management Agency, Independent Study Program, Course IS-235, "Emergency Planning*,*" *current edition*[12][13]

(~~v~~*w*) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980

(~~w~~*x*) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982

(~~x~~*y*) ~~Part~~ *Section* 1910.120 of title 29, Code of Federal Regulations

(~~y~~*z*) National Fire Protection Association Standard 472, "Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents," ~~2008~~ *current* ~~E~~*e*dition[13][14]

(~~z~~*aa*) National Fire Protection Association Standard 473, "Standard for Competencies for EMS Personnel Responding to Hazardous Materials/Weapons of Mass Destruction Incidents," ~~2008~~ *current* ~~E~~*e*dition [14][15]

(~~aa~~*ab*) Occupational Safety and Health Administration, "OSHA Best Practices for Hospital-Based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazard*ous* Substances," January 2005[15][16]

(~~ab~~*ac*) DoD Directive 7730.65, "Department of Defense Readiness Reporting System (DRRS)," June 3, 2002

(~~ac~~*ad*) DoD Instruction 6055.06, "*DoD* Fire and Emergency Services (F&ES) Program," December 21, 2006

(ae) Joint Publication 3-28, "Civil Support," September 14, 2007

(af) DoD Directive 3025.1, "Military Support to Civil Authorities (MSCA)," January 15, 1993

(ag) DoD Directive 3025.15, "Military Assistance to Civil Authorities," February 18, 1997

(~~ad~~*ah*) Title 32, United States Code

(~~ah~~*ai*) DoD Directive 5530.3, "International Agreements," June 11, 1987

---

[7][8] Available from http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf

[8][9] Available from https://hseep.dhs.gov/support/VolumeIII.pdf

[9][10] Available from http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[10][11] Available from http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[11][12] Available from http://training.fema.gov/EMIWeb/IS/is200.asp

[12][13] Available from http://training.fema.gov/EMIWeb/IS/is235.asp

[13][14] Available from http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=472

[14][15] Available from http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=473

[15][16] Available from http://www.osha.gov/dts/osta/bestpractices/html/hospital_firstreceivers.html

(~~ai~~*aj*)   Public Law 104-321, "Emergency Management Assistance Compact," October 19, 1996

(~~aj~~*ak*)   Public Law 103-160, "National Defense Authorization Act for Fiscal Year 1994," November 30, 1993

(~~ak~~*al*)   Executive Order 12196, "Occupational Safety and Health Programs for Federal Employees," February 26, 1980

(~~al~~*am*)   DoD Directive 4715.1E, "Environment, Safety, and Occupational Health (ESOH)," March 19, 2005

(~~am~~*an*) DoD Instruction 6055.1, "DoD Safety and Occupational Health (SOH) Program," August 19, 1998

(~~an~~*ao*)   DoD Instruction 6055.05, "Occupational and Environmental Health (OEH)," November 11, 2008

(~~ao~~*ap*)   Unified Facilities Criteria ~~4-021-01, "Design and O&M: Mass Notification Systems," April 9, 2008~~ *4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," January 22, 2007*[~~16~~*17*]

(~~ap~~*aq*)   DoD~~I~~ *Instruction* 6055.07, "Accident Investigation, Reporting, and Record Keeping," October 3, 2000

(~~aq~~*ar*)   Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," ~~as amended~~ *current edition*

[~~16~~*17*]Available ~~at~~*from* ~~http://www.wbdg.org/ccb/DOD/UFC/ufc_4_021_01.pdf~~ *http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf*

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) shall:

   a. Establish DoD-wide goals and objectives for the DoD IEM Program.

   b. Coordinate with the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) (ASD(HD&ASA)) on IEM matters of mutual interest.

   c. In coordination with the Under Secretary of Defense (Comptroller), provide criteria, guidance, and instruction to incorporate IEM program elements into appropriate DoD program and budget documents.

   d. Ensure synchronization of DoD IEM criteria, guidance, and instruction with DoD 3150.8-M and DoDD 3150.08 (References (f) and (g)).

2. DEPUTY UNDER SECRETARY OF DEFENSE FOR INSTALLATIONS AND ENVIRONMENT (DUSD(I&E)). The DUSD(I&E), under the authority, direction, and control of the USD(AT&L), shall:

   a. Develop policy and provide advocacy and oversight of the DoD IEM Program.

   b. Ensure that IEM programs are aligned and in accordance with title 10, United States Code (U.S.C.), and section 1522 of title 50, U.S.C. (References (h) and (i)) to provide the required standards for sustainment and life-cycle management.

   c. Conduct annual management reviews of each DoD Component's IEM Programs.

   d. Prepare and maintain DoD issuances, as needed, to provide specific policy, procedures, and standards to support the development, implementation, and sustainment of the DoD IEM Program, including the update and maintenance of this Instruction.

   e. Advocate for, resource, and support planning, programming, and budgeting processes for the DoD IEM Program.

   f. Advise USD(AT&L) on appropriate DoD-wide goals and objectives for the DoD IEM Program.

   g. Coordinate DoD IEM Program policy with appropriate OSD offices.

h. Establish a DoD EMSG comprised of members from OSD, the Joint Staff, the Military Departments, and the Defense Logistics Agency (DLA) to provide technical advice on IEM matters.

i. Appoint a representative to co-chair the DoD EMSG.

j. Participate in appropriate OSD-level committees, meetings, and working groups to represent IEM aspects related to installation protection, antiterrorism (AT), mission assurance, medical response, and critical infrastructure protection issues.

k. Request focused program evaluations of the DoD IEM Program from the DoD Inspector General as needed.

l. Develop, publish, and maintain, in coordination with appropriate OSD offices and the DoD Components, a definition of military-unique environments as it pertains to the use of military protective equipment for IEM.

m. Report annually to the USD(AT&L) on the status of the DoD IEM Program.

3. <u>ASSISTANT TO THE SECRETARY OF DEFENSE FOR NUCLEAR AND CHEMICAL AND BIOLOGICAL DEFENSE PROGRAMS (ATSD(NCB))</u>. The ATSD(NCB), under the authority, direction, and control of the USD(AT&L), shall develop policy and procedures consistent with References (h) and (i), national law, policy, and consensual standards for the acquisition, procurement, and sustainment of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) equipment.

4. <u>DIRECTOR, DEFENSE THREAT REDUCTION AGENCY (DTRA)</u>. The Director, DTRA, under the authority, direction, and control of the USD(AT&L), through the ATSD(NCB), *and in addition to the responsibilities in section 10 of this enclosure,* shall:

a. Serve as a technical advisor to the DoD EMSG.

b. Revise, coordinate, publish, employ, and maintain criteria for the evaluation of IEM capabilities based on the standards contained in this Instruction and integrate with the Joint Staff*/DTRA DoD* ~~Integrated~~ Vulnerability Assessment ~~(JSIVA)~~ ~~b~~*B*enchmarks.

c. Assess IEM capabilities as part of all ~~JSIVA~~ *Joint Staff/DTRA DoD Vulnerability Assessment Benchmarks*, *the* Defense Critical Infrastructure Program (DCIP) (DoDD 3020.40 and DoD Instruction (DoDI) 3020.45 (References (j) and (k))), and critical infrastructure assessments to determine compliance with this Instruction.

d. ~~Recommend incorporation of lessons learned from DoD IEM exercises and actual emergencies into applicable policy and procedures through the EMSG.~~ *Conduct analysis of IEM*

program data collected from assessments conducted by Joint Staff/DTRA DoD Vulnerability Assessment teams and provide a trends analysis briefing annually to the EMWG.

5. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) shall:

a. Develop, publish, and maintain human capital emergency preparedness guidance such as the Civilian Personnel Management Service Emergency Preparedness and Response Guide (Reference (l)).

b. Ensure the Armed Forces Chaplains Board, through the Deputy Under Secretary of Defense for Military Personnel Policy and in coordination with the Military Department training commands, includes early training for chaplains in mass casualty response and planning.

5~~6~~. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA)). The ASD(HA), under the authority, direction, and control of the ~~Under Secretary of Defense for Personnel and Readiness~~ *USD(P&R)*, shall:

a. Establish and maintain DoD-wide medical *(including mental health)* and public health goals and objectives for IEM programs.

b. In coordination with the DUSD(I&E), promote language in the Defense Planning *and Programming* Guidance ~~and the Defense Health Program~~ to ensure sufficient resources are allocated in the Military Departments' budgets to carry out the provisions of this Instruction.

c. Provide medical and public health expertise to the DUSD(I&E) for IEM.

d. Integrate Public Health EM initiatives with the DoD IEM Program such as emergency response, medical countermeasures (MCMs), public health emergencies, and medical surveillance.

e. Provide medical and public health policy pertaining to requests for assistance from foreign, Federal, State, local, and tribal governments prior to, during, or after an emergency.

f. Support DUSD(I&E) in developing and maintaining medical and public health IEM requirements for installation preparedness within an all-hazards framework and providing assistance to civil authorities during contingencies.

g. Establish a Medical EM Requirements Group to assist in the identification of installation medical and public health IEM requirements.

6~~7~~. <u>USD(P)</u>. The USD(P) shall develop DoD policy and provide oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government.

7~~8~~. <u>ASD(HD&ASA)</u>. The ASD(HD&ASA), under the authority, direction, and control of the USD(P), and as the focal point for Defense Support of Civil Authorities (DSCA)*, ~~and~~ DCIP, *and AT,* shall:

    a. Advise DUSD(I&E) on DSCA policy as it relates to IEM under mutual aid agreements (MAAs), memorandums of understanding (MOUs), and memorandums of agreement (MOAs).

    b. Support DUSD(I&E) in developing and maintaining IEM requirements for installation preparedness within an all-hazards framework and conducting civil support missions during contingencies.

    c. Provide policy and procedures on requests for IEM support from external sources (e.g., State, local, and tribal governments) prior to, during, or after an emergency.

    d. Serve as the DoD focal point for policy matters pertaining to homeland defense activities, DSCA matters with interagency partners, the Congress, State governments, local municipalities, and organizations in the private sector.

    e. Coordinate the development of DoD installation requirements related to homeland security and homeland defense missions, including the National Bio-Defense and the Domestic Nuclear Detection architectures, with appropriate OSD and interagency organizations including *the Office of the* DUSD(I&E).

    f. Serve as advisor for ~~domestic~~ AT as it relates to IEM according to DoDD 2000.12 (Reference (~~l~~*m*)).

    g. Advise DUSD(I&E) on critical assets located on installations.

    h. Ensure DCIP policy is synchronized with IEM policy.

    i. Serve as principle lead in the office of the USD(P) for IEM matters.

8~~9~~. <u>ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL ~~SECURITY~~ *STRATEGIC* AFFAIRS (ASD(GSA))</u>. The ASD(GSA), under the authority, direction, and control of the USD(P), and as the focal point for foreign consequence management (FCM); chemical, biological, radiological, and nuclear (CBRN) consequence management; and combating weapons of mass destruction, shall:

    a. Develop policy and provide procedures on the development of support agreements with host nations.

b. Advise DUSD(I&E) on FCM activities related to IEM for the Secretary of Defense.

c. Support DUSD(I&E) ~~in developing and maintaining~~ IEM requirements outside the United States ~~for installation preparedness within an all-hazards framework and assisting the~~ *with* host nation *assistance* during contingencies.

d. Advise DUSD(I&E) on policy pertaining to CBRN management.

~~9. ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS/LOW-INTENSITY CONFLICT AND INTERDEPENDENT CAPABILITIES (ASD(SO/LIC&IC)). The ASD(SO/LIC&IC), under the authority, direction, and control of the USD(P), shall advise DUSD(I&E) on global and nondomestic AT policy as it relates to IEM.~~

10. <u>HEADS OF THE DoD COMPONENTS</u>

a. The Heads of the DoD Components shall implement procedures for subordinate units that are tenants on installations, or supported commanders on joint bases, to fully participate in the respective installation's IEM Program.

b. The Heads of the DoD Components who manage installations shall:

(1) Implement IEM programs at their installations using the procedures for installation commanders in ~~paragraph~~ *section* 6 ~~of the main body~~ *above the signature of this Instruction,* ~~and~~ Enclosures 3 through 7*, and human capital requirements (e.g., implementation and practice of telework, the personnel accountability system, and safe haven procedures, as appropriate, in accordance with Reference (l))*.

(2) Plan, program, and budget for IEM requirements and execute IEM programs.

(3) Provide management support, resources, and staff to effectively implement IEM programs at all organizational levels.

(4) Ensure policy, procedures, and resources are available for the proper total life-cycle management (TLCM) of IEM equipment and facilities including acquisition, fielding, storage, and replacement functions.

(5) Designate, train, and resource an emergency program manager at the headquarters' level to support installation emergency managers administer their programs.

(6) Appoint a medical consultant at the headquarters' level to advise on medical and public health issues pertaining to the DoD IEM Program.

(7) Encourage installation commanders to seek EM Program certification.

(8) Assess IEM programs for compliance with requirements and effectiveness of execution.

(9) Participate in annual DUSD(I&E) management reviews.

11. <u>CHAIRMAN OF THE JOINT CHIEFS OF STAFF</u>. The Chairman of the Joint Chiefs of Staff shall:

a. Develop, publish, and maintain Joint doctrine and associated publications on the policy and tactics, techniques, and procedures necessary to implement the DoD IEM Program in the Joint environment.

b. Direct the Joint Requirements Oversight Council (JROC) to address IEM issues including the testing and evaluation of material solutions to support the rapid acquisition, fielding, and integration of both commercial and government technology for IEM.

c. Ensure the Chairman's program review and the Chairman's program analysis assessment include a summary of the DoD IEM Program requirements as determined by the DoD Components, the JROC, and integrated priority lists provided by the Combatant Commanders.

12. <u>COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS</u>. The Commanders of the Geographic Combatant Commands, through the Chairman of the Joint Chiefs of Staff *and in addition to the responsibilities in section 10 of this enclosure*, shall:

a. Support and assist U.S. civil authorities, as directed, in IEM activities for planning, preparing for, mitigating, responding to, and recovering from natural or manmade disasters or hazards.

b. Advocate for Service/Component IEM Program requirements through the program objective memorandum process.

c. Share results of risk management activities with installations within the Geographic Combatant Command's area of responsibility.

d. Ensure IEM requirements in foreign countries are executed in accordance with status-of-forces agreements (SOFAs) and applicable guidance relating to FCM *and humanitarian assistance and disaster relief operations*.

e. Integrate EM into their respective Combatant Command program reviews or similar programs.

13. <u>DoD EMSG</u>. The DoD EMSG shall:

   a. Consist of representatives from OSD offices, the Joint Staff, the Military Services, and ~~the~~ DL*A*.

   b. Recommend new and revised planning guidance and policy for all aspects of IEM.

   c. Meet semiannually, at a minimum, and at the call of the chairperson to share information, discuss items of mutual interest, and recommend policies and priorities on all aspects of IEM.

   d. Provide technical review of IEM issues at the request of OSD.

   e. Serve as the technical advisory board to the USD(AT&L) for the DoD IEM Program.

ENCLOSURE 3

DoD IEM PROGRAM EXECUTION

1. REQUIREMENTS. The requirements in this enclosure are implemented by installation commanders according to Enclosure 2, section 10.

2. CRITERIA

    a. The DoD IEM Program requirements contained within this Instruction align with References (b) and (d) and provide the DoD Components with guidance for implementing EM practices that are scalable, flexible, and adaptable to specific installation needs.

    b. The minimum required elements for an IEM Program contained in this Instru*c*tion are consistent with the guidance set forth in Reference (d) and provide the DoD Components with a structural framework that addresses and supports service EM guidance already in practice.

    c. For those installations that operate in the maritime domain, this aligns them with Maritime Operational Threat Response and Maritime Infrastructure Recovery Plan from the National Strategy for Maritime Security (References (~~m~~*n*) and (~~n~~*o*)).

3. IMPLEMENTATION PLAN

    a. Develop an IEM Program implementation plan addressing the necessary EM competencies and performance objectives.

    b. Employ a resource-balanced, phased implementation approach to ensure*:*

       (1) ~~i~~*I*nitial operational capability *(IOC)* within 2 years*. IOC includes completion of minimum tasks to enable installations worldwide to employ basic DoD IEM Program capabiltiies consistent with Federal, DoD, and DoD Component policy, guidance, and standards.*

       (2) ~~f~~*F*ull operational capability *(FOC)* within 5 years. *FOC includes completion of essential tasks to enable installations worldwide to employ and sustain DoD IEM Program capabiltiies consistent with Federal, DoD, and DoD Component policy, guidance, and standards.*

    c. Use the checklists provided in the appendix to this enclosure, which outline specific requirements for meeting IOC and FOC.

4. <u>FUNCTIONS</u>

    a. <u>Installation EM Working Group (IEMWG)</u>

        (1) Establish an IEMWG, under the direction of the installation commander, to meet at least quarterly. The IEMWG may be combined with existing working groups.

        (2) Ensure the activities associated with establishing and sustaining the IEM Program are performed in accordance with this Instruction.

        (3) Include, at a minimum, the installation commander or commander's representative, the program coordinator (e.g., the installation emergency manager), *senior installation chaplain,* and representatives from AT; CBRN; Medical; *Disaster Mental Health;* Safety; Public Health; Logistics; Legal; Security; Fire and Emergency Services (F&ES); Public Affairs; and tenant and subordinate commands and units.

    b. <u>Installation Emergency Manager</u>. Designate, in writing, an installation emergency manager to:

        (1) Employ resource management activities to coordinate the prioritization and allocation of resources at the installation including:

            (a) Development of resource management objectives that address:

                <u>1</u>. EM personnel, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the timeframe within which they are needed.

                <u>2</u>. Quantity, response time, capability, *capacity,* limitations, cost, and liability connected with using the resources.

                <u>3</u>. Resources and partnership arrangements essential to the IEM Program (e.g., MAAs, MOUs, MOAs).

            (b) Implementation of resource management procedures to locate, acquire, store, distribute, maintain, test, and account for personnel, services, resources, materials, and facilities procured or donated to the IEM Program that, at a minimum:

                <u>1</u>. Establish processes for describing, requesting, tracking, and taking inventory of resources.

                <u>2</u>. Activate these processes prior to and during an incident.

                <u>3</u>. Dispatch resources prior to and during an incident.

                <u>4</u>. Deactivate or recall resources during or after an incident.

5. Establish contingency planning for shortfalls of resources in accordance with NFPA 1600 (Reference (~~o~~*p*)).

(2) Develop and maintain the IEM Plan.

(3) Collaborate and coordinate with *Federal,* State, local, and tribal governments; other Military Department(s); and host-nation emergency managers to achieve the highest possible level of IEM Plan integration and interoperability.

(4) Coordinate with the *installation* medical treatment facility *emergency manager and public health emergency officer (PHEO)* to develop the IEM Plan and employ medical *and public health* resource management activities.

c. Personnel Categories. Use personnel categories (emergency responders, critical personnel, essential personnel, and other personnel) defined in DoDI 2000.16 (Reference (~~p~~*q*)) for the purpose of accurately identifying their protected population and effectively managing their personnel resources.

d. ~~IEETs~~ *Installation Exercise Evaluation Teams*

(1) Establish teams in sufficient numbers with resources to provide a means of periodically evaluating installation-level exercises.

(2) Evaluate the installation's capability to respond to incidents using an all-hazards EM approach.

(3) Include subject matter experts in EM including first responders who are familiar with Homeland Security Exercise and Evaluation Program (HSEEP), Volume III: Exercise Evaluation and Improvement Planning (Reference (~~q~~*r*)).

e. *Support Agreements. Where support agreements such as MOUs, MOAs, and MAAs exist at installations, establish procedures for the installation emergency manager to:*

(1) Maintain listings of all EM-related support agreements.

(2) Integrate MAAs and other support agreements into the IEM Plan.

(3) Ensure offices of primary responsibility review EM-related support agreements at a minimum annually, and when the ability to meet the requirements in the support agreements cannot be met. These reviews shall result in continuation, cancellation, or revision of the support agreement.

(4) Exercise support agreements annually, at a minimum.

5. <u>CREDENTIALING</u>

   a. Each DoD Component provides credentialing and documentation, consistent with their respective DoD Component guidance, that can authenticate and verify the certification and identification of designated responders. Installation commanders shall implement a credentialing process consistent with their Component's guidance.

   b. The DoD Component standards for credentialing and documentation must be consistent with guidance set forth in Federal Information Processing Standard 201-1 and Homeland Security Presidential Directive 12 (References (rs) and (st)). The credentialing of healthcare providers is governed by the ASD(HA) processes.

6. <u>CERTIFICATION</u>. Installation commanders are encouraged to seek IEM Program certification.

Appendix
   IEM Checklists

APPENDIX TO ENCLOSURE 3

IEM CHECKLISTS

Table 1. IOC Checklist

REQUIREMENTS	SEE DoDI REFERENCE
Establish a comprehensive all-hazards IEM program.	Enclosure 2, section 10.
Designate, train, and resource HQ-level EM program manager to support installation EMs.	Enclosure 2, subparagraph 10.b.(5)
Plan, program, and budget for IEM requirements and execute those requirements.	Enclosure 2, subparagraph 10.b.(2)
Adopt and implement procedures consistent with NIMS and ICS.	Paragraph 4.d. above the signature
Develop an HQ-level IEM implementation plan that addresses:	
1. Identification of Service-level procedures, guidance, and information requiring update or issuance.	Enclosure 4, paragraph 4.b.
2. Establishment of senior leader orientation.	Enclosure 5, paragraph 3.a.
3. Training requirements.	Enclosure 5, section 3.
4. Planning for reaching FOC by 2014.	Enclosure 3, paragraph 3.b.
Designate an HQ-level medical consultant to advise the IEM program.	Enclosure 2, subparagraph 10.b.(6)
Participate in the DoD EMSG.	Enclosure 2, section 13.
Designate an installation emergency manager.	Enclosure 3, paragraph 4.b.
Establish an IEMWG that meets quarterly, at a minimum.	Enclosure 3, subparagraph 4.a.(1)
Conduct a coordinated risk assessment that includes:	
1. Hazard/threat assessment.	Enclosure 4, subparagraph 3.b.(1)
2. Vulnerability assessment.	Enclosure 4, subparagraph 3.b.(2)
3. Capability assessment.	Enclosure 4, subparagraph 3.b.(3)
Develop and maintain an IEM plan.	Enclosure 4, section 4.
Develop an installation-level IEM program implementation plan that addresses:	
1. Establishment and/or review of support agreements.	Enclosure 3, paragraph 4.e.
2. Training.	Enclosure 4, subparagraph 4.b.(3)(d)
3. Exercises.	Enclosure 4, subparagraph 4.b.(3)(e)
4. Resource requirements.	Enclosure 3, paragraph 3.b.
Complete basic NIMS training requirements for personnel designated in the Service-level implementation plan.	Enclosure 5, paragraph 3.b.
Coordinate with State, local, and tribal governments.	Enclosure 3, subparagraph 4.b.(3)

Table 2. FOC Checklist

REQUIREMENTS	SEE DoDI REFERENCE
Services have implemented a process to assess the IEM program.	*Enclosure 2, subparagraph 10.b.(8)*
Service-level policy and guidance updated or issued.	*Enclosure 2, subparagraph 10.b.(8)*
Total life-cycle management of IEM equipment established and implemented.	*Enclosure 2, subparagraph 10.b.(4)*
IEM PROGRAM PLANNING	
Conduct a comprehensive risk management process annually that includes hazard and/or threat assessment, vulnerability assessment, and capability assessment.	*Enclosure 4, section 3.*
Coordinate, maintain, and update an all-hazards IEM plan annually that addresses and/or includes:	
1. Procedural compliance with NIMS and ICS.	*Enclosure 4, section 4.a.*
2. Deficiencies and lessons learned identified during exercises.	*Enclosure 4, paragraph 4.b.*
3. Considerations identified during risk management process.	*Enclosure 4, paragraph 4.b.*
4. Process to respond to increase or decrease in force protection condition.	*Enclosure 4, subparagraph 3.b.(2)*
5. Enhanced 911.	*Enclosure 4, subparagraph 4.b.(7)*
6. Integrated medical response actions within IEM in accordance with this Instruction.	*Enclosure 4, subparagraph 4.b.*
7. Necessary elements defined in this Instruction.	*Enclosure 4, paragraph 4.b.*
PREPAREDNESS	
Implement and maintain IEM training that satisfies the standards detailed in this Instruction.	*Enclosure 5, section 3.*
Implement an annual exercise and evaluation program that satisfies the standards detailed in this Instruction.	*Enclosure 5, section 4.*
Annually review and maintain support agreements.	*Enclosure 5, paragraph 5.a.*
Identify type and amount of equipment needed to support all-hazards response.	*Enclosure 5, section 6.*
Establish a life-cycle management process.	*Enclosure 2, subparagraph 10.b.(4)*
INCIDENT RESPONSE	
Develop all-hazards incident response measures consistent with OSHA requirements and in accordance with established criteria or guidance.	*Enclosure 6, section 2.*
Establish a well-defined communication plan that includes the capability to communicate within the Department of Defense and with emergency response personnel and local authorities.	*Enclosure 6, paragraph 2.b.*
Establish/activate an emergency operations center (EOC) that includes the ability to establish/share a common operating picture for emergency responders and local, State, DoD, and Federal authorities.	*Enclosure 6, subparagraph 2.b.(2)*
Apply ESF structure or equivalent functional area to installation emergency response and designate, in writing, an installation lead for each ESF/functional area	*Enclosure 6, paragraph 2.c.*

Table 2. *FOC Checklist, Continued*

REQUIREMENTS	*SEE DoDI REFERENCE*
INCIDENT RESPONSE (Continued)	
Maintain ability to warn/notify within 10 minutes of an incident:	
1. Personnel on-duty at the time of the incident.	*Enclosure 6, subparagraph 2.b.(2)(d)*
2. Base populace on installation at time of incident.	*Enclosure 6, subparagraph 2.b.(2)(d)*
3. Common facilities (e.g., schools, commissary, gym, community center).	*Enclosure 6, subparagraph 2.b.(2)(d)*
RECOVERY PHASE	
Maintain ability to establish a recovery working group and task it to:	
1. Conduct damage assessment.	*Enclosure 7, paragraph 2.b.*
2. Identify recovery priorities.	*Enclosure 7, paragraph 2.c.*
3. Manage fatalities.	*Enclosure 7, paragraph 2.e.*

ENCLOSURE 4

IEM PROGRAM PLANNING

1. <u>REQUIREMENTS</u>. The requirements in this enclosure are implemented by installation commanders according to Enclosure 2, section 10.

2. <u>PROCESS</u>. In the IEM Plan, define the vision, mission, goals, and objectives as they relate to the policy of the individual DoD Component. The planning process for all levels of command includes, but may not be limited to, risk management, IEM Plan development, and maintenance and reporting of accepted standards (e.g., Federal Emergency Management Agency IS-200.a and IS-235 (References (t*u*) and (u*v*)).

3. <u>RISK MANAGEMENT</u>

   a. Risk management is a comprehensive process and a critical planning element of IEM. The risk management process is performed and documented by the IEMWG under the authority of the installation commander and in coordination with functional areas such as AT, CBRN, and critical infrastructure protection (CIP). The completion of the risk management process will occur prior to the development of the initial IEM Plan or IEM Plan update and will be an ongoing process. Effective risk management will require the support of AT, Occupational Safety, Environmental Health, Public Works, Security, Information Technology, Logistics, Intelligence, Medical, F&ES, EM, and, as appropriate, State, local, and tribal governments, other Military Service(s), or host-nation partners in the local community. Successful risk management is dependent upon a comprehensive all-hazards risk assessment process, such as provided for in References (c) and (u*v*). The all-hazards risk assessment identifies and monitors hazards and threats and the likelihood of their *o*ccurrence, the vulnerability of the installation, and the consequences of those hazards and threats (Reference (o*p*)).

   b. Risk management methodologies consist of, at a minimum, the following types of assessments:

      (1) <u>Hazard and/or Threat Assessment</u>. All installations perform hazard and/or threat assessments in coordination with assessments performed for AT and critical infrastructure protection programs including assessments for criticality, hazards and/or threats, and vulnerability. Installations identify and/or address hazards and/or threats that have the potential to impact their installation. The hazard and/or threat assessment should consider all hazard and/or threat types and the likelihood of each type of hazard and/or threat occurring. Once identified, efforts to mitigate the potential effects of the identified hazards and/or threats or to prevent the hazard and/or threat from affecting the installation and its associated mission-essential functions are necessary. The appendix to this enclosure presents a list of hazards and/or threats to consider under the DoD IEM Program. The steps in hazard and/or threat assessment include:

(a) Identify and characterize the hazards and/or threats. Determine *specific hazards and/or threats,* if the installation is susceptible to natural disasters *be they natural events, human-caused events (accidental and intentional),* or *technologically caused events* and what additional hazards and/or threats they pose *may cause*.

(b) Consider the full range of known or estimated terrorist capabilities and possibilities of nonhostile incidents.

(c) Integrate threat information prepared by the intelligence community in liaison with Federal, State, and local law enforcement as appropriate and in accordance with restraints and procedures identified in DoDD 5200.27 or DoD 5240.1-R (References (v*w*) and (w*x*)).

(d) Evaluate each hazard for severity and frequency. Determine how often these hazards and/or threats affect the installation and what actions may help reduce their severity.

(e) Estimate the impact of the hazard and/or threat. Identify and quantify what missions or areas are potentially affected by these hazards and/or threats (consider special events).

(2) Vulnerability Assessment. All installations conduct vulnerability assessments in coordination with AT and DCIP programs and address the broad range of hazards and/or threats to the installation and its personnel using JSIVA *Joint Staff/DTRA DoD Vulnerability Assessment* bB*enchmarks, Service guidance, or Combatant Command guidance*.

(a) Consider the range of identified and projected response capabilities necessary for responding to any type of hazard and/or threat.

(b) Identify the appropriate course of action to address vulnerabilities and solutions for enhanced protection of DoD personnel and resources.

(c) Include identified defense industrial base and DCIP assets.

(d) Provide a vulnerability-based analysis of the installation's critical assets. Identify potentially exploited vulnerabilities and suggest options for eliminating or mitigating the exploitation of those vulnerabilities.

(3) Capability Assessment. All installations performing *shall conduct* capability assessments should *and* consider contingency planning activities. The objectives of the capability assessment are to:

(a) Consider the range of identified and projected response capabilities necessary for responding to any type of hazard.

(b) List installation resources by type to provide an asset capability report.

(c) Review policy, guidance, and planning documents to identify the organization's mission essential tasks (METs) and functions assigned to the organization.

(d) List installation personnel with an MET EM responsibility as identified in Enclosure 3, paragraph 4.c.

(e) Identify costs associated with assessment outcomes for future budget planning.

c. Additional assessments should leverage AT and DCIP efforts and include, but not be limited to, critical infrastructure, infrastructure interdependency, consequence, criticality, and needs assessments.

d. The vulnerability assessments described in this Instruction are conducted and validated annually, prior to the update or review of the IEM Plan. The results of the assessments determine the basis and justification for IEM Program enhancements, program planning, and budget requests using ~~JSIVA~~ *Joint Staff/DTRA DoD Vulnerability Assessment* ~~b~~*B*enchmarks*, Service guidance, or Combatant Command guidance*.

4. <u>IEM PLAN</u>. An all-hazards IEM Plan developed and maintained at each installation should be designed to support pre-incident *preparedness* planning, mitigation, emergency response, and recovery. The IEM Plan must be flexible enough for use in all emergencies, including unforeseen events, yet detailed enough to provide a course of action for installation commanders to proceed with preplanned responses to an unexpected event.

a. <u>NRF and NIMS</u>. In accordance with Reference (e), the Department of Defense implements policy and procedures consistent with the roles and authorities under the NRF. The NRF establishes clear objectives for a concerted national effort to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other domestic emergencies. The NRF, using NIMS principles, provides the structure and mechanism for a consistent, nationwide approach for Federal, State, and local governments to effectively and efficiently work together to manage domestic incidents regardless of cause, size, or complexity. IEM Plans are developed to ensure procedural compliance with NIMS and ICS. To the extent possible, installations outside the United States should consider NRF and NIMS principles when implementing their IEM programs.

b. <u>IEM Plan Elements</u>. IEM Plans assign responsibilities to organizations and individuals and support areas of pre-incident planning, emergency response, medical and public health needs, *disaster mental health,* equipment, law enforcement, training, intelligence support, *religious support,* security, ~~response,~~ and recovery. IEM Plans are coordinated with other protection-related program plans including, but not limited to, AT, physical security, F&ES, environmental, and hazardous materials (HAZMAT). At a minimum, IEM Plans are updated annually and incorporate lessons learned and opportunities for improvement identified during exercises and risk management activities. All IEM Plans are developed in accordance with this Instruction which aligns with NRF and NIMS concepts and addresses, at a minimum, the following:

(1) Mission, goals, and objectives of the IEM Program.

(2) Functional roles, responsibilities, and lines of authority for all personnel, organizations, and agencies assigned EM response.

(3) Preparedness activities including:

(a) Risk management.

(b) Prevention planning that establishes interim and long-term actions to reduce and/or eliminate identified hazards and/or threats to the installation.

(c) Mitigation planning that establishes interim and long-term actions to reduce the impact of hazards and/or threats that cannot be eliminated.

(d) Training.

(e) Exercises.

(f) Interagency coordination.

(g) Equipment.

(4) Response planning that establishes response actions and assigns responsibilities for carrying out those actions. Specific response planning considerations include:

(a) Continuity of operations planning that identifies mission essential *functions and* personnel, procedures, and resources as well as contact information of stakeholders to be notified, critical and time-sensitive applications, alternative work sites, processes, and functions to be maintained while the installation is recovering.

(b) Evacuation management and mass care planning that addresses the mass care concept, family assistance, sheltering-in-place, *lockdown,* local and remote safe havens, civilian shelter, personnel accountability, special needs management, and animal needs management.

(c) Volunteer and donations management that establishes procedures for all IEM Plans for organizing and coordinating the receipt of unsolicited services and/or goods in a manner that comports with applicable law and policy and does not interfere with ongoing response and recovery efforts.

(d) Family Assistance Center crisis and mass casualty response that establishes procedures to integrate victim and family services in response to the full spectrum of crisis or catastrophic events.

(e) Crisis and mass casualty response that integrates religious support in response to the full spectrum of crisis or catastrophic events.

(f) Appropriate dynamic protocols to allow non-DoD first responders to access the installation in an emergency.

(5) Recovery planning that provides short-term and long-term priorities for restoration of functions, services, resources, facilities, programs, and infrastructure.

(6) Communications through all phases of an emergency that address communication capability and operation of major communication nodes ~~such as~~ *to include, but not be limited to,* dispatch centers, mobile command posts, *and* incident command~~s vehicles and services with recording capability for each installation either direct support (government owned and operated) or in general support from another organization off installation~~.

c. <u>IEM Plan Structure</u>. The IEM Plan structure should be written to address the three phases of incident management per the NRF: prepare, respond, and recover. The annexes should address the hazards that threaten the installation.

5. <u>ENHANCED 911</u>. All installations shall have:

a. The availability of enhanced 911 services with recording capability at domestic installations through either direct support (Government-owned and -operated) or support from State and local authorities off the installation.

b. Requirements to subscribe for enhanced 911 services for Voice-Over Internet Protocol users and emergency dispatch capabilities for nondomestic installations.

Appendix
  Hazard Identification List

APPENDIX TO ENCLOSURE 4

HAZARD IDENTIFICATION LIST

Table 3. DoD IEM Hazard Identification List

Natural Hazards	
Geological Hazards	Earthquake, tsunami, volcano, landslide, mudslide, subsidence, glacier, iceberg, etc.
Meteorological Hazards	Flood, flash flood, seiche, tidal surge, drought, fire (forest, range, urban, wild land, urban interface), snow, ice, hail, sleet, avalanche, windstorm, tropical cyclone, hurricane, tornado, water spout, dust or sand storm, extreme temperature (heat, cold), lightning strikes, ~~famine,~~ geomagnetic storm, etc.
Biological Hazards	Diseases that impact humans or animals such as plague, ~~smallpox,~~ anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (also known as SARS), pandemic disease, bovine spongiform encephalopathy (also known as mad cow disease), etc.
Human-Caused Events	
Accidental	HAZMAT (e.g., explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, radiological, corrosive) spill or release; explosion or fire; transportation accident; building or structure collapse; energy, power, or utility failure; fuel or resource shortage; air or water pollution or contamination; dam, levee, or other water control structure failure; financial issues including economic depression, inflation, financial system collapse; communication system interruption; misinformation; etc.
Intentional	Terrorism (CBRNE and cyber), sabotage, civil disturbance, public unrest, mass hysteria, riot, enemy attack, war, insurrection, strike or labor dispute, disinformation, criminal activity (vandalism, arson, theft, fraud, embezzlement, data theft), electromagnetic pulse, physical or information security breach, workplace violence, *active shooter,* product defect or contamination, harassment, discrimination, etc.
Technologically Caused Events Affecting the Following	
Central computer, mainframe, software, or application (internal and external)	
Ancillary support equipment	
Telecommunications	
Energy, power, or utility	

~~Source: Reference (o).~~

ENCLOSURE 5

PREPAREDNESS

1. <u>REQUIREMENTS</u>. The requirements in this enclosure are implemented by installation commanders according to Enclosure 2, section 10.

2. <u>INTRODUCTION</u>. Preparedness consists of all activities taking place prior to the onset of an emergency to prepare categorized personnel, installation tenants, and the base population for the eventual response to, and recovery from, an emergency. These activities include planning, education and training, exercises and evaluations, interagency coordination, and procurement of emergency response equipment.

3. <u>TRAINING</u>. An education and training program is developed and implemented to create awareness across the installation and enhance the skills of individuals assigned EM functions or responsibilities. The DoD Components develop training curriculum and educational materials to ensure an appropriate level of competency for installation commanders, responders, technicians and specialists, and the base population. At a minimum, IEM education and training encompasses the following:

   a. <u>Senior Leader Orientation</u>. Develop, implement, and sustain a senior leader orientation program. This program provides senior leaders with the requisite knowledge to implement IEM Program policies, facilitate oversight of all aspects of subordinate IEM programs at the strategic and operational levels, and support mitigation, preparedness, prevention, response, and recovery operations conducted at their subordinate commands.

   b. <u>IEM Program Manager and Installation Emergency Manager Training</u>. Ensure appropriate training of designated IEM program managers and installation emergency managers tasked with overseeing and implementing IEM programs and plans. IEM program managers and installation emergency managers shall be fully trained in appropriate NIMS, NRF, *HSEEP,* ICS (~~e.g.~~ *i.e.*, ICS 100, 200,~~700~~ *300, 400*) and EM ~~concepts~~ *fundamentals, principles,* and policies in order to fulfill the responsibilities of this role.

   c. <u>Emergency First-Responder and First-Receiver Training</u>. At a minimum, provide all emergency first responders and receivers with appropriate ICS, emergency medical services (EMS), HAZMAT, and task-specific training. All EMS and HAZMAT training should be in accordance with part 1910.120 of title 29, Code of Federal Regulations (Reference (~~x~~*y*)); NFPA Standards 472 and 473 (References (~~y~~*z*) and (~~z~~*aa*)); and Occupational Safety and Health Administration's (OSHA) "OSHA Best Practices for Hospital-Based First Receivers of Victims from Mass Casualty Incidents Involving the Release of Hazardous Substances" (Reference (~~aa~~*ab*)). Emergency first-responder and first-receiver training in areas outside the United States needs to be consistent with appropriate host-nation first-responder and receiving elements according to applicable agreements (SOFA, etc.).

d. <u>Community Awareness</u>. Ensure IEM community awareness and emergency preparedness information is made available to all assigned personnel, including family members, upon indoctrination and on an annual basis or more frequently as the local threat situation dictates.

e. <u>New Equipment Training</u>. As new IEM equipment is deployed, train personnel assigned EM responsibilities requiring use of the new equipment in accordance with Service policy and procedures regarding new equipment.

f. <u>HSEEP</u>. Ensure all members of the IEET are familiar with HSEEP, a capabilities and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning. HSEEP courses are available online at https://hseep.dhs.gov/pages/1001_HSEEP7.aspx.

g. <u>Training Exercises</u>. For purposes of training, ensure, at a minimum, annual participation in ~~DoD and/or national exercises relevant to IEM~~ *an exercise and/or case study of a hazard from the Appendix to Enclosure 4*.

h. <u>Tracking and Reporting</u>. Ensure the lead functional area for each MET tracks the training provided to personnel. Reporting is accomplished in accordance with DoDD 7730.65 (Reference (~~ab~~*ac*)) and may be augmented by DoD Component-specific policy and procedures.

4. <u>EXERCISES</u>. The DoD Components implement an exercise and evaluation program for installations under their control. Exercises:

a. Assess and validate EM proficiency levels, clarify and familiarize EM personnel with roles and responsibilities, improve interagency coordination and communication, highlight capability gaps, and identify opportunities for improvement.

b. Include multidiscipline, multijurisdictional incidents.

c. Include participation of appropriate leaders and decision-makers representing each of the emergency response functions on the installation and whenever possible, appropriate State, local, and tribal governments; other Military Department(s); and host-nation, private-sector, and nongovernmental organization (NGO) partners.

d. Assess the following components of the IEM Plan and/or EM response capabilities:

(1) Activation of local support agreements (e.g., MAAs, MOUs, MOAs, SOFAs).

(2) Execution of notification protocols, both internal (installation personnel, including tenant organizations, only) and external (with Higher Headquarters, State, local, and tribal governments, other Military Department(s), and host-nation partners).

(3) Mass warning and notification.

(4) Command, control, and communication.

(5) First-responders and first-receivers.

(6) Emergency operators and specialists.

(7) Medical response *(includes disaster mental health)*.

(8) Religious support response.

(9) Family assistance response.

e. ~~Should~~ *Shall* be conducted annually, at a minimum. EM exercises may be conducted in coordination with, or as a part of other, tabletop, full-scale, or functional exercises (e.g., AT and force protection exercises). Certain functions of the IEM Plan such as shelter-in-place, continuity of operations, and mass warnings and notification should be conducted semiannually, one in conjunction with or as part of a tabletop, full-scale, or functional exercise. The other semiannual exercise can be a stand-alone event aimed at sustaining proficiency and building skills prior to an installation's annual exercise.

f. Include a thorough and objective exercise evaluation process. During the exercise and upon its conclusion, the evaluation team, functional participants, and leadership evaluate performance against relevant capability, identify deficits, and institute after-action reporting. After-action reporting and improvement planning develop specific recommendations for changes in practice, timelines for implementation, and assignments for completion, including incorporation of lessons learned into the annual IEM Plan update and review process.

g. Contain a mechanism for incorporating corrective actions through the development of an after-action report. At the end of each exercise, DoD installations conduct a formal review among exercise participants and observers of EM actions performed successfully, outcomes achieved, lessons learned, and areas for improvement derived from the exercise. Upon completion of the after-action reports, a corrective action plan is developed and implemented and the results incorporated into the annual IEM Plan review and update process. After-action reports shall be kept for at least 2 years.

5. <u>INTERAGENCY COORDINATION</u>. All IEM programs coordinate, where appropriate, with State, local, and tribal governments, other Military Department(s), or host-nation emergency response agencies and departments to identify and update responsible points of contact, emergency protocols, and expectations in the event of an emergency on or impacting a DoD installation in accordance with References (~~o~~*p*), (~~p~~*q*), and DoDI 6055.06 (Reference (~~ac~~*ad*)). Such coordination should include the sharing of information pertaining to deployed technologies and capabilities that may provide early warning of a potential hazard or threat (e.g., bio-monitoring; chemical, radiological, and/or nuclear detection; intrusion detection; decision support systems).

a. <u>Support Agreements</u>. Installation commanders develop or provide input to support agreements with local emergency services, including local EM agencies. These support agreements include MAAs or other support agreements written as an MOA, MOU, inter-Service support agreement, SOFA, or support contracts. Installation legal counsel assists in the preparations and performs a legal review of all support agreements before execution.

b. <u>DSCA</u>.

(1) Response action(s) fall under the rules in Joint Publication 3-28 and DoDDs 3025.1 and 3025.15 (References (ae), (af), and (ag)):

(a) If the response includes U.S. Federal military forces; National Guard forces performing duty under title 32, U.S.C. (Reference (~~ad~~*ah*)); DoD civilians; DoD contract personnel; and DoD Component assets and

(b) Is in response to requests for assistance from Federal, State, local, and tribal governments for domestic emergencies, designated law enforcement support, and other domestic activities.

(2) Support provided by National Guard forces performing duty under Reference (~~ad~~*ah*) is considered DSCA but is conducted as a State-directed action.

c. <u>Overseas</u>. All overseas installations coordinate their efforts with the supported Geographic Combatant Command and, consistent with Geographic Combatant Command guidance, with appropriate Department of State officials and host nations in accordance with DoDD 5530.3 (Reference (~~ah~~*ai*).

d. <u>EM Assistance Compact (EMAC)</u>. EMAC shall not be used for the coordination, deployment, and/or utilization of military equipment or personnel. In accordance with Public Law 104-321 (Reference (~~ai~~*aj*)), EMAC coordinates MAA and partnership between States and may be used for the exchange and sharing of any response or recovery capability. EMAC is applicable to DoD civilian and contractor response and recovery assistance. The entry point into EMAC for IEM programs is through the State EM agency's designated contact in accordance with Reference (~~ai~~*aj*).

e. <u>Immediate Response Rule</u>. In accordance with References (af) and (ag), commanders may provide immediate assistance to civil authorities. This form of immediate assistance (the "immediate response rule") is employed only when the need to save lives, prevent human suffering, or mitigate great property damage is a direct concern. The commander must then report the incident to higher headquarters as soon as possible.

f. <u>Emergency Public Information (EPI)</u>. Installations are responsible for the provision of accurate and verifiable EPI to their protected population prior to, during, and after an emergency. In the event of an emergency, DoD installations ensure the timely communication of pertinent information such as conveying impacts and analyses of the incident. Additionally, DoD

installations provide opportunities for stakeholders to provide information on community impacts, lessons learned, and other relevant information from the community; supporting Federal, State, local, and tribal governments; other Military Department(s); host-nation partners; the media; and members of the general public.

    g. Interoperability. IEM programs should be consistent with EM efforts in their civilian mutual aid community or host nation in order to ensure an effective and efficient emergency response. The interoperability requirements of equipment, communication systems, and other EM capabilities are identified and improved through interagency collaboration, coordination, and participation in all aspects of EM. Interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. EM interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with information assurance.

6. EQUIPMENT. Determine the type and amount of equipment needed to support capabilities for emergency response on installations under their control. Equipment requirements should consider factors such as priority, objective-level of response capability, and the hazards, threats, and vulnerabilities identified during the risk management activities. Not all installations will require the same type or amount of equipment. Ensure that equipment needs are identified for each installation using a process that is flexible enough to accommodate the needs of specific installations, while at the same time standardizing emergency response capabilities and providing cost-effective solutions that provide a minimal level of EM capability at each installation. Consider closing equipment gaps using agreements for support with the local community EM units when possible.

    a. Equipment Standards. Equipment standards include both government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) solutions to equipment requirements.

        (1) GOTS and COTS equipment used to detect the presence of, protect against the effects of, or remove or reduce the hazard of CBRN agents are procured, maintained, employed, and inventoried in accordance with Public Law 103-160 (Reference (~~aj~~*ak*)) and applicable Joint Chemical Biological Defense Program, Joint Requirements Office, Joint Program Executive Office for Chemical and Biological Defense, and Service guidance.

        (2) Equipment worn by emergency first responders complies with Executive Order 12196 (Reference (~~ak~~*al*)), OSHA regulations, and National Institute for Occupational Safety and Health guidelines pertaining to HAZMAT response, as appropriate and in accordance with DoDD 4715.1E and DoDIs 6055.1 and 6055.05 (References (~~al~~*am*), (~~am~~*an*), and (~~an~~*ao*)).

        (3) The DoD Chemical and Biological Defense Non-Standard Equipment Review Panel serves as a basis for the selection of CBRN-related COTS equipment. COTS equipment validation for use by Military Departments is completed as required.

b. <u>TLCM</u>. Maintain equipment replenishment and disposal in accordance with the equipment's specified life cycle. Assure appropriate funding for the maintenance and accountability of the equipment including sustainment training, certification, equipment upgrades, replacement, and expendables for all installations under their control.

c. <u>Equipment Interoperability</u>. Ensure, when possible, that installation emergency response equipment is interoperable with equipment used by mutual aid partners in the local communities.

ENCLOSURE 6

INCIDENT RESPONSE

1. <u>REQUIREMENTS</u>. The requirements in this enclosure are implemented by installation commanders according to Enclosure 2, section 10.

2. <u>MEASURES</u>. Develop all-hazards incident response measures consistent with OSHA requirements and in accordance with established criteria or guidance. The measures include procedures for establishing incident command to coordinate security, F&ES, medical, HAZMAT, and other emergency responders. The IEM Plan should include first-responder and first-receiver standard operating strategies or procedures to execute their capabilities to rescue personnel, prevent human suffering, or stop the loss or damage caused by the incident while continuing essential installation operations. Each installation response occurs under different circumstances and involves different response actions. Installations must rely on their own resources, MAAs *and other support agreements*, SOFAs, and Federal, State, local, NGO, and host-nation resources and capabilities to respond. Ensure that appropriate IEM response capabilities include:

   a. <u>Event Triggers</u>. An initial event or series of events results in a "trigger" that sets in motion a series of response actions. Triggers may be the result of a natural hazard or a signal received from deployed detection equipment, medical surveillance information, visual, and/or intelligence analysis. The types of detection technologies deployed at installations may vary, however, at a minimum, installations shall have access to:

      (1) <u>Health Threat Surveillance and Detection</u>. The medical official or designee:

         (a) Identifies all medical and public health information needed, such as syndromic surveillance, and provide all-hazards health protection.

         (b) Ensures laboratory support to confirm and identify hazardous substances in the affected environment.

         (c) Integrates and monitors surveillance systems operations.

         (d) Monitors the health status of essential personnel and the general population.

      (2) <u>Medical Intelligence</u>. The public health or medical functional area designee, through direction of the medical commander, receives, extracts, and/or collects information from available medical sources, provides medical information to local organizations and private sector partners, and works to sustain information and/or intelligence-gathering activities necessary for assessing and/or reassessing emerging health threat information during an incident.

(3) <u>Intelligence Sharing and Dissemination</u>. Installations shall identify multiple intelligence sources both within and outside the Department of Defense (e.g., the general public, military intelligence, national intelligence institutions, and local and host-nation law enforcement intelligence) and establish and agree upon the following:

(a) Intelligence information and products that will not be shared under any circumstances with EM organizations outside the Department of Defense.

(b) Intelligence information and products that will be shared only with a human-in-the-loop "pushing" the intelligence information and products to EM organizations outside the Department of Defense who have been authorized to receive intelligence information and products.

(c) Intelligence information and products that will be shared without a human-in-the-loop based upon prior agreement with an authorized EM organization outside the Department of Defense.

(d) Intelligence information and products that can be obtained through an open source.

b. <u>Command, Control, and Communication</u>. Installations shall have a well-defined communication plan that includes the capability to communicate within the Department of Defense, with personnel engaged in the response, as well as with civil authorities. Command, control, and communication management establishes:

(1) <u>ICS</u>. Per Reference (e), DoD installations adopt procedures consistent with ICS principles for all emergencies covered by the DoD IEM Program.

(2) <u>Emergency Operations Center (EOC)</u>. EOCs ~~represent the physical location~~ *are the distinctive locations* where the coordination of information and resources to support the incident commander occur. The EOC is activated to support on-scene response during an escalating incident by relieving the burden of external coordination and securing additional resources. The EOC consists of personnel and equipment appropriate for the level of incident and can manage multiple incidents and planned events. All EOCs have standard operating procedures for monitoring incident development and provide the following functionality or capability:

(a) <u>Common Operating Picture</u>. The EOC uses a common operating picture and information management system in order to execute and support actions ~~listed in~~ *required by* the IEM Plan*, support the incident commander,* and facilitate coordination of incident information.

(b) <u>Interoperable Communications</u>. The EOC ensures interoperable communications that support Service Component's first-responder and first-receiver missions and are encouraged to ensure interoperable communications with civil authorities.

(c) <u>Continuous Warning Point</u>. The Heads of the DoD Components ensure a continuous capability that serves as the contact or warning point for emergency situations.

(d) Mass Warning and Notification.

1. At a~~A~~ll DoD installations, ~~develop~~ *shall maintain* mass warning and notification capabilities ~~with the ability~~ to warn all personnel ~~within~~ *immediately, but no longer than* 10 minutes ~~of~~ *after* incident notification *and verification* ~~at the dispatch center~~ . ~~Mass warning and notification capabilities are developed in accordance with Unified Facilities Criteria 4-021-01 (Reference (ao)). All mass warning and notification systems are tested regularly, unless restricted by local or host-nation ordinances.~~

2. All DoD installations shall possess, operate, and maintain, or have dedicated access to, communications capabilities at the EOC or other centralized location to ensure mass warning and notification.

3. The mass warning and notification must give response direction using intelligible voice communications, visible signals, text, text messaging, computer notification, tactile, or other communication methods.

4. Mass warning and notification systems installed interior to buildings shall comply at a minimum with the requirements of Unified Facilities Criteria 4-010-01 (Reference (ap)).

(e) Communicate CBRN Detection Incidents. At all DoD installations, develop a process for ensuring information dissemination of a detected CBRN incident to appropriate organizations and agencies including, but not limited to, the intelligence community, law enforcement personnel, and responders, according to existing protocols.

c. Emergency Support Functions (ESFs). ESFs outlined in the NRF organize and provide structure to Federal interagency emergency response activities. Installations apply the ESF structure or equivalent functional areas to installation emergency response and assign personnel to lead or manage a specific ESF functional area. Areas designated for installations include:

(1) ESF 1 – Transportation.

(2) ESF 2 – Communications.

(3) ESF 3 – Public Works and Engineering.

(4) ESF 4 – Firefighting.

(5) ESF 5 – EM.

(6) ESF 6 – Mass Care, Emergency Assistance, Housing, and Human Services.

(7) ESF 7 – Logistics Management and Resource Support.

(8) ESF 8 – Public Health and Medical Services.

(9) ESF 9 – Search and Rescue.

(10) ESF 10 – Oil and HAZMAT Response.

(11) ESF 11 – Agriculture and Natural Resources.

(12) ESF 12 – Energy.

(13) ESF 13 – Public Safety and Security.

(14) ESF 14 – Long-Term Community Recovery.

(15) ESF 15 – External Affairs.

   d. <u>Medical Response</u>. Medical response actions are a critical component of any response. Where medical capabilities exist, the IEM Program accounts for the following medical response actions:

      (1) <u>Direct and Conduct Health Threat Surveillance and Investigation Operations</u>. The ~~public health or medical functional area~~*PHEO or his or her* designee:

         (a) Directs and supports inspections and investigations of suspected sources of health threats.

         (b) Prioritizes health surveillance activities and makes force health recommendations.

         (c) Coordinates Public Health EM resources to perform inspection and surveillance activities.

         (d) Identifies and directs compliance of applicable laws, policies, and implementation procedures governing dissemination of information.

         (e) Conducts investigations and analyzes results for health threats.

         (f) Performs increased surveillance and disease investigations based on how much higher the disease and nonbattle injury rates are compared to the reference (local) standards.

         (g) Recommends health control measures based upon investigations.

      (2) <u>Confirm and Characterize Impact of Threats</u>. The ~~public health emergency officer~~ *PHEO* or public health functional area designee assesses the health impacts of all-hazards agents on personnel and environment.

      (3) <u>Develop and Maintain Plans, Procedures, Programs, and Systems</u>. The ~~public health or medical functional area~~ *PHEO or his or her* designee uses appropriate surveillance tools and

mechanisms to develop, coordinate, and maintain plans, procedures, programs, and systems that detect, identify, quantify, and communicate effective health threat surveillance and support.

    (4) <u>Develop a Mass Prophylaxis Plan</u>. DoD Installations develop a mass prophylaxis plan for ensuring the distribution of MCMs during a public health emergency. The plan specifies the installation's inherent capability and those of supporting resources (e.g., civilian institutions, local health departments, or access to the Strategic National Stockpile). Medical Logistics tracks mass prophylaxis and other medical supplies.

    (5) <u>Provide Patient Care</u>. The medical commander or public health designee:

        (a) Executes patient care plans and medical MAAs *and other support agreements*.

        (b) Coordinates, manages, and provides health services, including first-responder capabilities, emergency care, mass casualty care, triage, first-receiver care, patient movement, psychological support, and pharmacy, dental, and veterinary services.

        (c) Develops patient care, fatality management, and healthcare system evacuation plans and procedures appropriate in all-hazards responses (including mass casualty, isolation, and quarantine incidents).

        (d) Develops medical MAAs *and other support agreements* for medical facilities and equipment.

        (e) Develops and maintains a deployable patient care capability.

ENCLOSURE 7

RECOVERY PHASE

1. <u>REQUIREMENTS</u>. The requirements in this enclosure are implemented by installation commanders according to Enclosure 2, section 10.

2. <u>ACTIONS</u>. Recovery activities often extend long after the incident itself. Short-term recovery actions seek to restore lifeline systems (e.g., power, communication, water and sewage, and transportation) and ensure that the needs of individuals and the community are met (e.g., maintain the rule of law, provide crisis counseling, demonstrate that people do care and that help is coming). Once some level of stability is achieved, the installation can begin restoring operations, rebuilding destroyed property, and reconstituting government operations and services. If applicable, commanders will coordinate with local, regional, and national authorities for Maritime Infrastructure Recovery Planning as delineated in Reference (~~n~~*o*). During the recovery phase, the installation:

    a. <u>Establishes a Recovery Working Group (RWG)</u>. An RWG shall be established early in the recovery phase of every emergency where, in the judgment of the Commander, recovery operations require coordination. If applicable, RWG will coordinate with local, regional, and national authorities on the restoration of maritime infrastructure per Reference (~~n~~*o*). The RWG is a task-organized working group focused on the evaluation, prioritization, and coordination of recovery requirements.

    b. <u>Conducts Damage Assessments</u>. The Public Works Civil Engineering asset may conduct physical damage assessments, if such a capability exists within the installation. All installations with Public Works Civil Engineering capabilities should develop an organic damage assessment capability and limited debris clearance capabilities. These capabilities should support short-term (less than 2 weeks in duration) recovery efforts and initial damage assessments, resource projections, and recovery planning requirements.

    c. <u>Identifies Recovery Priorities</u>. Installation commanders establish recovery priorities consistent with the installation mission. Consideration is given to operational mission priorities and re-establishment of the normal operating environment.

    d. <u>Conducts Recovery Planning</u>. The RWG (formed post-incident), with the technical direction of the installation emergency manager and the installation Public Works Civil Engineering representative, conducts recovery planning at the installation level. While the IEM Plan facilitates response and short-term recovery, the recovery plan provides detailed, incident-specific processes and procedures including immediate restoration of transportation and communication capabilities, search and rescue operations, utility reconstructions, community reconstructions, site remediations, medical care *(to include mental health)* or mitigations, and other activities necessary for successful long-term recovery.

e. <u>Ensures Effective Fatality Management and Mortuary Affairs</u>. The installation emergency manager will coordinate with appropriate functional areas to establish procedures for ensuring effective fatality management. All fatality management activities are sufficiently documented and incorporated in the surveillance and intelligence-sharing networks to identify sentinel cases of other public health threats, including bioterrorism. Fatality management includes:

(1) Scene documentation, collection, and recovery of human remains, personal effects, and items of evidence.

(2) Decontamination of remains and personal effects (if required).

(3) Transportation, storage, documentation, and recovery of forensic and physical evidence.

(4) Determination of the nature and extent of injury.

(5) Identification of fatalities, certification of the cause and manner of death, processing, and returning human remains and personal effects to legally authorized persons.

(6) Interaction with and provision of required legal, customary, compassionate, and culturally competent services to the family of the deceased.

(7) Coordination with the civil law enforcement, public health, and medical authorities to perform these functions when capabilities do not exist at the installation.

f. <u>Continues Communication</u>. The need for EPI does not end immediately after the response phase as there is a continued need to exchange information with the full range of affected populations during the recovery phase. DoD installations continue communication during recovery operations by providing pertinent information to all stakeholders.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(GSA)	Assistant Secretary of Defense for Global Security Affairs
ASD(HA)	Assistant Secretary of Defense for Health Affairs
ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
~~ASD(SO/LIC&IC)~~	~~Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities~~
AT	antiterrorism
ATSD(NCB)	Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CIP	critical infrastructure protection
COTS	commercial-off-the-shelf
DCIP	Defense Critical Infrastructure Program
DLA	Defense Logistics Agency
DSCA	Defense Support of Civil Authorities
DTRA	Defense Threat Reduction Agency
DUSD(I&E)	Deputy Under Secretary of Defense for Installations and Environment
EM	emergency management
EMAC	emergency management assistance compact
EMS	emergency medical services
EMSG	Emergency Management Steering Group
EOC	emergency operations center
EPI	emergency public information
ESF	emergency support function
F&ES	fire and emergency services
FCM	foreign consequence management
FOC	*full operational capability*
GOTS	government-off-the-shelf
HAZMAT	hazardous materials
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	incident command system
~~IEET~~	~~Installation Exercise Evaluation Team~~
IEM	installation emergency management

IEMWG	Installation Emergency Management Working Group
IOC	*initial operational capability*
JROC	Joint Requirements Oversight Council
~~JSIVA~~	~~Joint Staff Integrated Vulnerability Assessment~~
MAA	mutual aid agreement
MCM	medical countermeasure
MET	mission essential task
MOA	memorandum of agreement
MOU	memorandum of understanding
NFPA	National Fire Protection Association
NGO	nongovernmental organization
NIMS	National Incident Management System
NPG	National Preparedness Guidelines
NRF	National Response Framework
OSHA	Occupational Safety and Health Administration
PHEO	*public health emergency officer*
RWG	Recovery Working Group
SOFA	status–of-forces agreement
~~TCA~~	~~task critical asset~~
TLCM	total life-cycle management
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	*Under Secretary of Defense for Personnel and Readiness*

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

all-hazards. Any incident, natural or manmade, including those defined in DoDI 6055.07 (Reference ~~ap~~*aq*)), that warrants action to protect the life, property, health, and safety of military members, dependents, and civilians at risk, and minimize any disruptions of installation operations.

AT. As defined in Joint Publication 1-02 (Reference (~~aq~~*ar*)).

awareness level. The ability to recognize that an incident is occurring and to initiate an emergency response sequence by notifying proper authorities. Awareness level requires no further action beyond notifying the authorities.

capability assessment. A DoD, command, or unit-level evaluation (assessment) to identify capabilities for responding to a natural or manmade disaster or hazard.

casualty management. A process by which coherent and interrelated sets of procedures, policies, and plans are developed in order to optimize the baseline capability to deal with patient populations expected in a mass casualty incident. Effective casualty management includes the efficiency to increase capacity during the response to a mass casualty incident.

common operating picture. A continuously updated overview of an incident compiled throughout an incident's life cycle from *standard data (meaning standard data elements, definitions, etc.) shared between integrated and compatible* systems *(meaning systems that can talk to each other)* for communication, information management, and intelligence and information sharing. The common operating picture ~~allows incident managers at all levels to make effective, consistent, and timely decisions~~ *facilitates collaborative planning and assists all echelons to achieve situational awareness*. The common operating picture ~~also helps ensure~~ *provides* consistency at all levels of incident management across jurisdictions, as well as between various governmental jurisdictions and private-sector and nongovernmental entities ~~that are engaged~~.

consequence management. As defined in Reference (~~aq~~*ar*).

continuity of operations. As defined in Reference (~~aq~~*ar*).

criticality assessment. As defined in Reference (~~aq~~*ar*).

critical personnel. Personnel deemed necessary for ensuring that a military mission identified as being "critical" is performed.

DCIP. A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the national military strategy.

DSCA. Support provided by U.S. Federal military forces, National Guard forces performing duty under Reference (~~ad~~*ah*), DoD civilians, DoD contract personnel, and DoD Component assets, in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities. Support provided by National Guard forces performing duty under Reference (~~ad~~*ah*) is considered DSCA but is conducted as a State-directed action.

EM. See Introduction, Framework Unpacked, page 5 of Reference (d).

enhanced 911 capability. A telephone system consisting of network, database, and enhanced 911 equipment that uses the single three-digit number "911" for reporting police, fire, medical, or

other emergency situations to a central location, while automatically associating a physical address with the calling party's telephone number.

ESFs. Used by the Federal Government and many State governments as the primary mechanism at the operational level to organize and provide assistance. ESFs align categories of resources and provide strategic objectives for their use. ESFs use standardized resource management concepts such as typing, inventorying, and tracking to facilitate the dispatch, deployment, and recovery of resources before, during, and after an incident. DoD is considered a support agency to all ESFs.

essential personnel. Personnel deemed necessary for ensuring that a military mission identified as being "essential" is performed.

evacuation management. Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas.

FCM. As defined in Reference (~~aq~~*ar*).

first receivers. Employees at a hospital engaged in decontamination and treatment of victims during an emergency incident occurring at a site other than the hospital. These employees are a subset of first responders.

first responders. Firefighters, law enforcement and/or security personnel, emergency medical technicians, and explosive ordnance disposal personnel who provide the initial, immediate response to an all-hazards incident.

full-scale exercise. Full-scale exercises simulate a real event as closely as possible. They are exercises designed to evaluate the operational capability of EM systems in a highly stressful environment that simulates actual response conditions. To accomplish this realism, they require the mobilization and actual movement of emergency personnel, equipment, and resources as outlined in the IEM Plan. Full-scale exercises incorporate the EOC and installation support functions.

functional exercise. Functional exercises are designed to validate and evaluate individual capabilities, multiple functions, activities within a function, or interdependent groups of functions. Events are projected through an exercise scenario with event updates that drive activity at the management level. Functional exercises simulate the reality of operations in a functional area by presenting complex and realistic problems that require rapid and effective responses by trained personnel in a highly stressful time-constrained environment.

hazard assessment. A DoD, command, or unit-level evaluation (assessment) to identify hazards and associated risk to person, property, and structures and to improve protection from natural or manmade disasters or hazards. Hazard assessments serve as one of the foundational components for effective EM activities including planning, resource management, capability development, public education, and training and exercises.

HSEEP. A *Department of Homeland Security* capabilities and performance-based exercise program that provides a standardized methodology and terminology for exercise design, development, conduct, evaluation, and improvement planning.

ICS. As defined in Reference (~~aq~~*ar*).

incident. An occurrence or event, natural or manmade, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wild land and urban fires, floods, HAZMAT spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, medical and public health emergencies, and other occurrences requiring an emergency response.

incident commander. The person identified in the IEM plan who has overall authority and responsibility for the management of all incident operations.

installation. ~~An installation is defined as a grouping of facilities located in the same vicinity, which support particular functions under the direction of a single commander.~~ *A base, camp, post, station, yard, center, or other activity under the jurisdiction of the Secretary of a Military Department, or, in the case of an activity in a foreign country, under the operational control of the Secretary of a Military Department or the Secretary of Defense. For the purpose of this Instruction, the term installation does not include leased facilities.*

interoperability. The ability of EM and response personnel to interact and work well together. In the context of technology, interoperability also refers to having an emergency communications system that is the same or is linked to the same system that a jurisdiction uses for nonemergency procedures, and that effectively interfaces with national standards as they are developed. The system should allow the sharing of data with other jurisdictions and levels of government during planning and deployment.

long-term recovery. See Chapter II: Response Actions, page 45, of Reference (d).

MAA. Written agreement between and among agencies and organizations and/or jurisdictions that provides a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

Military Services. As defined in Reference (~~aq~~*ar*).

mitigation. Activities providing a critical foundation in the effort to reduce injuries and the loss of life and property from natural and/or manmade disasters by avoiding or lessening the impact of a disaster.

NGO. An entity with an association that is based on interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with government.

Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross. NGOs, including voluntary and faith-based groups, provide relief services to sustain life, reduce physical and emotional distress, and promote the recovery of disaster victims. Often these groups provide specialized services that help individuals with disabilities. NGOs and voluntary organizations play a major role in assisting emergency managers before, during, and after an emergency.

NIMS. System that provides a proactive approach guiding government agencies at all levels, the private sector, and NGOs to work seamlessly to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.

NPG. Guidance that establishes a vision for national preparedness and provides a systematic approach for prioritizing preparedness efforts across the nation. The NPG focus policy, planning, and investments at all levels of government and the private sector. The NPG replace the Interim National Preparedness Goal and integrate recent lessons learned.

NRF. Guides how the Nation conducts all-hazards response. The NRF documents the key response principles, roles, and structures that organize national response. It describes how communities, States, the Federal Government, and private-sector and nongovernmental partners apply these principles for a coordinated, effective national response. It describes special circumstances where the Federal Government exercises a larger role, including incidents where Federal interests are involved and catastrophic incidents where a State would require significant support. It allows first responders, decision-makers, and supporting entities to provide a unified national response.

operational level. The ability to initially respond to an incident for the purpose of protecting nearby persons, the environment, or property.

preparedness. The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and coordination among government, private-sector, and NGOs to identify threats, determine vulnerabilities, and identify required resources. Within NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

private sector. Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry.

recovery. See Chapter II: Response Actions, page 45 of Reference (d).

resource management. A system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover

from an incident. Resource management includes MAA and other assistance agreements; the use of special Federal, State, tribal, and local government teams; and resource mobilization protocols.

risk assessment. A process of qualitatively or quantitatively determining the probability of an adverse event and the severity of its impact on an asset. It is a function of threat, vulnerability, and consequence.

risk management. A continual process or cycle where risks are identified, measured, and evaluated; countermeasures are then designed, implemented, and monitored to see how they perform, with a continual feedback loop for decision-maker input to improve countermeasures and consider tradeoffs between risk acceptance and risk avoidance.

tabletop exercise. An exercise that facilitates the analysis of an emergency situation in an informal, stress-free environment. These exercises are designed to elicit constructive discussion as participants examine and resolve problems based on an existing EM Plan and identify where the plan needs to be refined.

threat. An indication of possible violence, harm, or danger.

threat assessment. A DoD, command, or unit-level evaluation (assessment) to identify threats to an installation, unit, exercise, port, ship, residence, facility, or other site to natural or manmade disasters or hazards.

United States. The several States, the District of Columbia, the Commonwealths of Puerto Rico and the Northern Mariana Islands, American Samoa, Guam, Midway and Wake Islands, the United States Virgin Islands, any other territory or possession of the United States, and associated navigable waters, contiguous zones, and ocean waters of which the natural resources are under the exclusive management authority of the United States. Also included are the Federated States of Micronesia and the Republic of the Marshall Islands.

vulnerability assessment. A DoD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to natural or manmade disasters or hazards. Vulnerability assessments identify areas of improvement to withstand, mitigate, and deter such hazards and serve as one of the foundational components for effective EM. The vulnerability assessment should address the broad range of hazards and threats to the installation and its personnel including but not limited to food, water CBRNE, and CIP assessments.